COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

March 4, 2014

TO: Mitchell H. Katz, M.D., Director
Department of Health Services

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – HARBOR-UCLA MEDICAL CENTER**

We have completed a review of the Department of Health Services (DHS) Harbor-University California, Los Angeles Medical Center's (Harbor-UCLA) compliance with the Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic Clinical Health (HITECH) Act.[1] On January 22, 2014, we provided your Department with our final draft report, and your Department agreed with our findings. No exit conference was requested.

Approach/Scope

The purpose of the review was to evaluate Harbor-UCLA's compliance with HIPAA and the HITECH regulations, including best practices and relevant County and Departmental policies and procedures. The scope of this review included the *HIPAA Privacy Rule and HITECH Act Audit Tool*, which is a general assessment to determine whether Harbor-UCLA is compliant with privacy, security, training, policies and procedures, and breach notification requirements.

Our review covered the Privacy Rule requirements for: 1) notice of privacy practices (NPP) for protected health information (PHI), 2) safeguards for privacy protections for PHI, 3) workforce member access to PHI, 4) administrative requirements, 5) disclosures of PHI, 6) amendment of PHI, 7) accounting of disclosures, and 8) the interim requirements for the HITECH Act's Breach Notification Rule. The review also covered certain privacy and security cross-over areas of the Security Rule, which include administrative, physical, and technical safeguards.

[1] 45 Code of Federal Regulations (CFR) Parts 160 and 164

To assist us with this review, we met with representatives from Health Services Administration (HSA), DHS' Privacy Officer, Harbor-UCLA's Director of Health Information Management (HIM), and Harbor-UCLA's Director of Information Systems Administrative Services.

Results of Review and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.[2]

Our review found that Harbor-UCLA posted its NPP in all designated waiting areas where patients are likely to view it. The NPP is current and includes the correct information on patient HIPAA rights, as well as the contact information for the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the County's Chief HIPAA Privacy Officer. Posting the NPP is crucial to promoting the awareness of HIPAA privacy rights related to services received at Harbor-UCLA. It also satisfies the HIPAA Privacy Rule's physical posting of the NPP requirement.

In addition, the HIPAA Privacy Rule requires covered entities that maintain a website to prominently post their NPP on their website.[3] We reviewed the Harbor-UCLA website in November 2013, and noted that it included a link to its NPP in both English and Spanish.

Notices of Privacy Practices Acknowledgement of Receipt

A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgement of receipt of the notice only at the time the provider first gives the notice to the individual (i.e., at first service delivery).[4]

It appears that Harbor-UCLA is compliant with the NPP Acknowledgement of Receipt standards. We randomly selected and reviewed 20 patients' medical charts to determine whether Harbor-UCLA obtained patients' acknowledgement of receipt of the NPP. All charts reviewed included the acknowledgement of receipt documentation.

---

[2] 45 CFR §164.520(c)
[3] 45 CFR §164.520(c)
[4] 45 CFR §164.520(c)(2)

Physical Safeguards

A covered entity must have in place appropriate administrative and physical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI (ePHI), and make reasonable efforts to prevent any intentional or unintentional use or disclosure that is in violation of the Privacy Rule.

It appears that Harbor-UCLA is compliant with the physical safeguards' standards that we reviewed. During the review, we found that computer monitors that were in public areas were positioned away from the public's view so that the information was not readable. Fax machines, printers, and copiers were kept in secure areas and away from visitors. The public did not have access to non-public areas of the hospital, outpatient clinic, and administrative offices.

The medical records' room is located in a stand-alone building and is operational at all times. The HIM Director told us that only authorized workforce members have access to the area, which is secured with a keypad at the entrance. This site is in accordance with the HIPAA Privacy Rule and it appears that appropriate physical safeguards are met, and in compliance with the regulations.

Administrative Safeguards for PHI

HIPAA requires that covered entities have in place appropriate administrative, technical, and physical safeguards for PHI. Specific guidance as to what constitutes appropriate safeguards is provided in the Security Rule. However, the Privacy Rule, which extends to non-electronic information, does not define reasonable or appropriate. As such, in implementing reasonable safeguards, Harbor-UCLA must analyze its needs and circumstances, such as the nature of the PHI, and assess the potential risks to patients' privacy.

During our review, we found that Harbor-UCLA's pharmacy provides patients with a number and displays the number on a marquee to notify patients that their medications are ready. This method of notification is in compliance with the Administrative Safeguards and reasonably protects the patient's privacy.

Minimum Necessary Rule

The Privacy Rule requires covered entities to make reasonable efforts to limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose of the disclosure. The OCR allows covered entities flexibility to address their unique circumstances, and make their own assessment of what PHI is reasonably necessary for a particular purpose.[5] As of the date of this report, the

[5] 45 CFR §164.502 and 514(d)

minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes.

We reviewed DHS' current policy, which addresses the HIPAA standards on the Minimum Necessary Rule. Discussions with DHS and Harbor-UCLA management indicate that workforce members are aware of the minimum necessary standards and to the best of their ability they adhere to them. They are further aware that the standards do not apply in certain situations, such as for treatment or when disclosures are required by law. Harbor-UCLA also has a *Minimum Necessary* policy that provides procedures for routine and non-routine requests to disclose PHI and it too addresses the HIPAA standards on the Minimum Necessary Rule.

Training

A covered entity must train all members of its workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules, to the extent necessary and appropriate for the members of its workforce to carry out their functions. Members of the workforce include workforce members, volunteers, and trainees.[6]

During the review, we were informed that all Harbor-UCLA workforce members have received training on HIPAA, the HITECH Act Breach Notification Rule, and DHS' HIPAA policies and procedures. New-hire training is handled by DHS' Human Resources Division through the orientation process. Existing DHS and Harbor-UCLA workforce members also receive classroom training, and are directed to review the on-line training materials offered on DHS' Intranet website. Upon the workforce member's completion of the HIPAA training, Harbor-UCLA manually documents and logs it in their central training database noting that the workforce member received HIPAA training.

We reviewed Harbor-UCLA's training records, and found that 70 (1.8%) out of 3,859 workforce members have not completed the required HIPAA training. Note that of the 70 employees that have not completed the training, 68 are inactive (i.e., on leave) and two employees are new-hires scheduled to take the training within the 30-day of hire timeframe. This is reasonable, acceptable per policy, and within the federal and State statutory requirements on training personnel prior to permitting them access to PHI.

Given the above indicators regarding Harbor-UCLA's training and the fact that 68 employees are inactive and two active employees are within the 30-day allocated timeframe for taking the training, it appears that Harbor-UCLA is compliant with the HIPAA training standards.

[6] 45 CFR §164.530(b)

Complaint Process

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received, and their disposition, if any.[7]

According to Harbor-UCLA's HIM Director, if a patient or visitor wants to file a complaint, they are directed to the Patients' Advocates Office located in the main hospital, where the complainant receives a "Grievance Form". Complaints are assessed to determine the type of complaint (e.g., health and safety, privacy, security, or other), and Harbor-UCLA will attempt to resolve all complaints within five business days. If additional time is needed to resolve the complaint, patients will be contacted in writing. In addition to having a complaint process, Harbor-UCLA's NPP states how and where an individual may file a complaint with DHS' Privacy Officer, the County's Chief HIPAA Privacy Officer, and/or OCR.

It appears that Harbor-UCLA has a complaint process and a policy (Harbor-UCLA Policy 728, *Complaints Related to the Privacy of Protected Health Information*) that meet the HIPAA standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with Harbor-UCLA management confirm their awareness and understanding of the requirement to adhere to Harbor-UCLA's non-retaliation policy. Further, they understand that OCR will investigate any complaint against a covered entity that engages in retaliatory actions. It appears that Harbor-UCLA's Policy 710, *Non-retaliation,* is compliant with the HIPAA retaliatory acts' standard.

Uses and Disclosures Requiring an Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

Discussions with Harbor-UCLA's management and Privacy Officer confirm that their workforce members have a general understanding of DHS' policy regarding uses and disclosures requiring an authorization from patients or their legal representatives. Our

[7] 45 CFR §164.530(d)

review of Harbor-UCLA's *Authorization for Use and Disclosure of Protected Health Information* form shows that it meets the HIPAA required elements.

It appears that Harbor-UCLA is compliant with the uses and disclosures requiring an authorization standard.

Accounting of Disclosures of PHI

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity. Covered entities must account to individuals for certain non-routine disclosures of PHI, and the Privacy Rule allows individuals to receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure. Disclosures that are not required to be reported include: to the individual; for treatment, payment, and health care operations; for facility directories; pursuant to authorization; pursuant to a limited data set agreement; to persons involved in the individual's care; for correctional institutions; and, certain law enforcement purposes.

Harbor-UCLA does not manually maintain an accounting of disclosures for patients. Instead, all disclosures are tracked systematically by the Affinity Information Technology system. Harbor-UCLA management reported that they have never received a request for an accounting of disclosures since the Privacy Rule became effective in April 2003. In the event HHS modifies its accounting of disclosures standard to include all disclosures of PHI to be part of the medical record, Harbor-UCLA management indicated that they are able to accommodate the changes.

It appears that Harbor-UCLA is compliant with the accounting of disclosures of PHI standard.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers, health plans, and other entities covered by HIPAA to notify individuals when their health information is breached. These "breach notification" regulations implement provisions of the HITECH Act. The regulations, developed by the OCR, require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Harbor-UCLA management told us that they follow DHS' Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI),* which provides procedures for workforce members when they

encounter a potential privacy and/or security breach. DHS' Policy 361.11 combines investigation procedures, the complaint process, and instructions on how to report a breach in one document. Harbor-UCLA also developed and follows Policy 737 *Security Incident Report and Response*, covering the breach notification process in the event there is an information technology breach.

Technical Safeguards

HIPAA requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form.[8] This means that DHS must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware of electronic media on which it is stored.[9]

Harbor-UCLA and DHS have policies to safeguard PHI and ePHI. In addition, Harbor-UCLA has a policy requiring that computers be password protected, and management indicated that system controls have been put in place to require password changes every 90 days, and to automatically log users out after five minutes of inactivity. Workforce members are frequently reminded to protect their passwords, to not share their passwords with anyone, and to not store PHI on hard drives. Additionally, the level of access to patients' electronic medical records is determined and granted based on the workforce member's role and business need to know and have such access.

To the extent that we were able to review Harbor-UCLA's technical safeguards' policies, their policies appear to comply with the HIPAA and HITECH standards.

Appropriate Access to ePHI

The Security Rule requires covered entities to have policies and procedures to ensure that workforce members have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI.[10]

DHS' Policy 935.15, *System Audit Controls*, addresses controls to record and examine system activity for all electronic information systems. DHS stated that access to its applications require users to authenticate to the system, and that they maintain session logs, rights, and other tools to ensure appropriate access to the system's data. DHS' Policy 935.14, *System Access Controls*, addresses the requirement to preserve and protect the confidentiality, integrity, and availability of ePHI on DHS networks, systems, software programs, for those workforce members that have access rights.

[8] 45 CFR §164.530(c)
[9] 45 CFR §164.310(d)
[10] 45 CFR §308(a)(3)(i)

According to DHS, current user accounts are established upon completion and approval of the required access request forms. However, DHS is in the process of merging DHS' directory services with the countywide standard, MS Active Directory, which is hosted by the Internal Services Department. Upon completion, user accounts will be created for new workforce members in eCAPS. When a workforce member terminates service with DHS, the Department will process the appropriate forms to delete the member's account, and the user will no longer have network access.

To the extent that we were able to review Harbor-UCLA's Systems Controls' policy and procedures, it appears they are compliant with this standard.

Contingency Plan

The Security Rule includes requirements for covered entities to ensure the confidentiality, integrity, and availability of all ePHI information they create, receive, maintain, or transmit. The Security Rule further requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Other provisions require policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. Contingency plans must be implemented and tested.[11]

DHS' Policy 935.07, *Facility IT Contingency Plan*, details the requirements that Harbor-UCLA must follow to be compliant with HIPAA regulations. In addition, DHS indicated that a new data center located at the Martin Luther King, Jr., Multi-Service Ambulatory Care Center campus will maintain facility back-up computer applications. DHS is in the process of replacing the existing Affinity Health Information System applications with a fault tolerant consolidated enterprise Affinity system. Further, as part of its disaster recovery plan, DHS contracts with a vendor who transports back-up tapes to a secure location. It appears that DHS' Policy 935.07, *Facility IT Contingency Plan*, addresses the Security Rule standard.

Proper Destruction of PHI

Covered entities must implement reasonable safeguards to limit incidental and prohibited uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the Security Rule requires implementation of policies and procedures to address the final disposition of ePHI and/or the hardware and electronic media on which PHI is stored.[12]

DHS' Policy 935.13, *Device and Media Controls*, addresses proper disposal of ePHI. The policy states that "prior to disposal or transfer of IT resources out of DHS' inventory,

[11] 45 CFR §164.308(a)
[12] 45 CFR §§164.310(d)(2) and 164.530(c)

all information and software containing PHI shall be rendered unreadable and unrecoverable to prevent unauthorized disclosure of DHS data". It appears that DHS' Policy 935.13, *Device and Media Controls,* is compliant with this standard.

Conclusion

Our review shows that Harbor-UCLA management, and specifically their Privacy and Security Officers, have a good understanding of the HIPAA Privacy and Security Rules' regulations and standards. As a result, Harbor-UCLA's HIPAA compliance program has benefited. We appreciate the opportunity to review the Harbor-UCLA facility and interview its workforce members in order to ensure continued HIPAA and HITECH Act compliance with the regulations. We also wish to thank HSA and Harbor-UCLA staff who participated in the review for their cooperation.

Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

WLW:RGC:GZ:LTM

c: William T Fujioka, Chief Executive Officer
Gregory Polk, Deputy, Chief Executive Office
Robert Pittman, Chief Information Security Officer, Chief Information Office
Stephanie Reagan, Principal Deputy County Counsel, County Counsel
Audit Committee
Health Deputies